User Guide

© Sistech 1999 - 2003

Contents

1 Introduction....3
1.1 Why and how to use e-mail encryption....3
1.1.1 Why use encryption....3
1.1.2 How it works....3
1.2 Functionalities....5
2 Getting started....7
2.1 Installing....7
2.2 Possible problems during installation....8
3 How to use....9
3.1 CryptoMailer User Interface....9
3.2 List of attached files....10
3.2.1 Right Mouse click and Double-click....10
3.2.2 Adding files that are already encrypted to the list....10
3.3 Message text field....12
3.4 Entering a Passphrase....13
3.4.1 Manual editing ("Manual")....13
3.4.2 Passphrases and labels (identifiers)....13
3.4.3 Passphrase Management (« List... »)....13
3.5 Passphrase Management....15
3.5.1 Removing a Passphrase....15
3.5.2 Exporting Passphrases....16
3.5.3 Importing Passphrases....17
3.6 Encrypt and Send....19
3.6.1 Sending an encrypted e-mail....19
3.6.2 Encrypt locally....20
3.6.3 Temporary decryption (Open)....21
3.6.4 Decrypt locally....21
3.6.5 Replying to an encrypted mail....21
3.7 User authentication....22
3.8 Self-Extracting File....24
3.9 Encryption algorithms....25
3.10 System menu....27
3.11 Drag and Drop....28
3.12 Context Menu....29
3.13 Receiving an encrypted file....29
3.14 Opening an encrypted file....30
3.15 Problems with encrypting files....30
4 Uninstalling....31
4.1 Start Menu....31
4.2 Control Panel....31
5 CryptoBoard....32
5.1 Introduction....32
5.2 Mechanisms....32
6 Contacts....33

© Sistech 1999 - 2003

1 Introduction

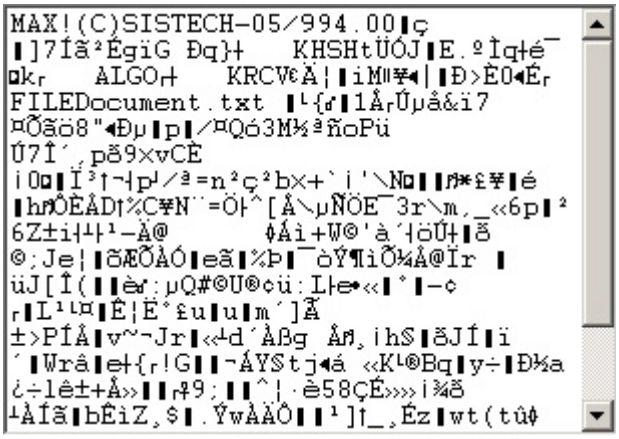
1.1 Why and how to use e-mail encryption

1.1.1 Why use encryption

E-mails are being sent from computer to computer without any protection regarding the information transmitted. E-mails are exactly like Postcards and can be read by virtually everybody.

Your colleagues, your corporate Network administrator, your ISP, relay servers on the internet, the ISP at the receiving end, his colleagues, his Network administrator are all capable to spy on your e-mail messages.

CryptoMailer provides an easy to use and most efficient way to keep anybody from spying on your e-mail. By using CryptoMailer, your e-mail is encrypted and anybody spying on your messages will only see something similar to this :



All the information you send or receive with CryptoMailer is encrypted and can not be read by any unauthorized person.

1.1.2 How it works

Each time CryptoMailer encrypts an e-mail or a file, a random number is generated. This random number is protected by a secret key being derived from the encryption Passphrase provided by the user.

By using this mechanism, the encrypted document or e-mail generated by CryptoMailer will be different each time, even if you encrypt the same document with the same Passphrase several times. This mechanisms provides an exceptionally high resistance to cryptanalysis, making it virtually impossible for anybody who does not know the Passphrase to decrypt or « crack » the encrypted documents.

By consequence, the only way to decrypt a document or e-mail encrypted by CryptoMailer is by using the correct Passphrase or through a « Brute Force Attack » (trying all possible combinations of the binary encryption key).

Brute Force

A person or organization intercepting an encrypted message may use to recover the encrypted information by « Brute Force ». This method implies trying all possible combinations of character chains (potential Passphrases). Provided that the user has chosen a sufficiently complex Passphrase, Brute Force requires an extremely high amount of time and processing capacity, making it virtually impossible to recover an encrypted message without knowing the Passphrase beforehand.

© Sistech 1999 - 2003

Given a Passphrase like "k5L;@y=P" containing 8 characters, a potential hacker will need to test all possible combinations of character strings (notwithstanding that he/her would not know the length of the Passphrase used) in order to find the right one.

Given that there are 112 characters and signs on a computer Keyboard, there are 2,5 x 10^e16 (25 million billions) to test. Given that the hacker has access to processing power enabling him / her to check one million combinations per second, it would take him / her about 800 years to check all possible combinations.

Rather than trying to find the Passphrase, a potential hacker might try to directly find the binary encryption key. This key is 128 bits in size, representing 2exp128 possible combinations (= 3,4 x 10^e+38). This represents far more combinations than the Passphrase itself. Even with a processing power of one billion computers, with each computer being able to check one billion combinations per second, the chances for finding the right key value before the definite extinction of the sun (in about 4,5 billion years) remains lower than 1 % !

Dictionary

For practical reasons, only few people actually choose Passphrases like « k5L;@y=P". Therefore, hackers usually use electronic dictionaries in order to create Passphrases based on common terms and expressions.

Using a dictionary attack, a hacker does not check a random number of characters, but rather complete words and expressions : all the words of the English (or any other) language), all first names and family names, etc. and all possible combinations with numbers. Using this kind of approach, expressions like « Melinda » and « ashtray » will systematically be checked, as well as for example, « Melinda37 », as well as all possible birthday combinations over the last 70 or so years.

Such dictionaries can easily be found for most languages on the Internet. Given that an average dictionary contains 50000 expressions, if you are using common expressions to build a Passphrase, a combination of at least 3 different expressions provides a reasonable level of security.

There are actually 2,5 billion of possible combinations for a Passphrase based on 2 out of 50.000 expressions. Using a computer system capable of testing one million combinations per second, it would take less than 42 minutes to check all possible combinations.

Therefore, even though the Passphrase contains more characters, a phrase like « "Thank God it's Friday » provides a much lower level of protection than "k5L;@y=P".

Anyhow, a Passphrase like « Thank God it's Friday » certainly provides a reasonable level of security ; Except if this particular expression represents a « verbal phrase » in the corresponding language or if it corresponds to any particular habits of the user. In that case, his / her colleagues and family members might be able to take an easy guess. … !

Recommendations

It is highly recommended to apply a minimum of security rules when you define a Passphrase.

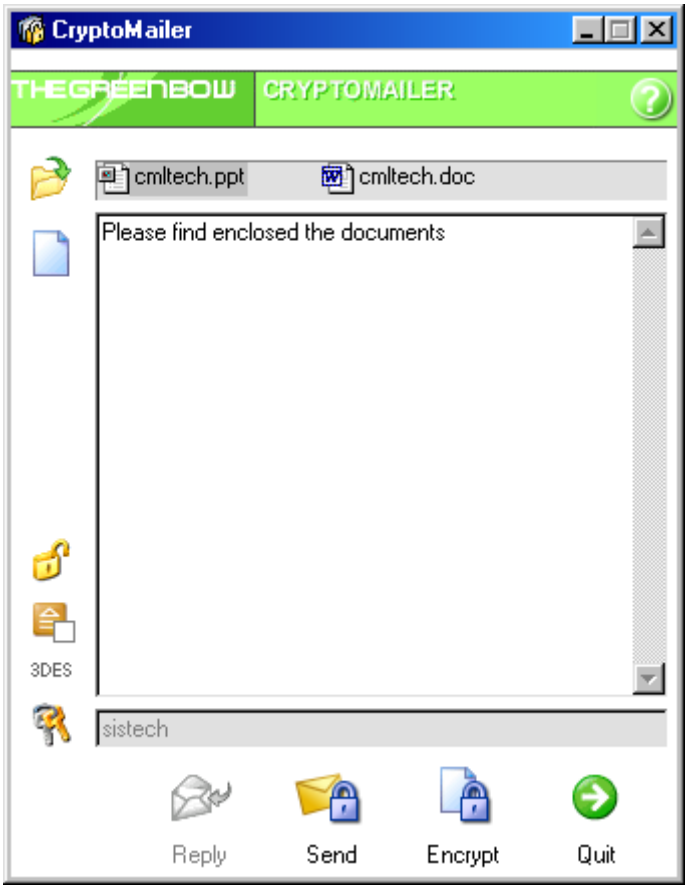
© Sistech 1999 - 2003

1.2 Functionalities

CryptoMailer is an encryption tool specially designed to be user-friendly : In less than one minute you can install the program and send your first encrypted message.

1 Download and Install CryptoMailer
2 Drag a file and add your text
3 Choose a Key
4 Send your first encrypted email
1 minute

CryptoMailer provides Drag&Drop support, context menu in Explorer (right mouse button) and starts automatically when you click on an encrypted message in your mail client. CryptoMailer is based on standard 3DES or AES 128bit encryption for file attachments and text messages.



© Sistech 1999 - 2003

Fast installation and user friendly key management make it possible to send your first encrypted e-mail in less than one minute.

CryptoMailer is specially designed for maximum compatibility with all mail clients (Outlook, Lotus Notes, Netscape Messenger, Eudora, Pegasus, etc...). Messages encrypted with CryptoMailer can be decrypted with the free of charge READER. Cryptomail-Reader is available for free download at www.thegreenbow.com.

Using symmetric cryptographic algorithms, CryptoMailer is based on shared secrets. The Passphrase list can be imported or exported safely (the Export file being encrypted). When receiving an encrypted message, CryptoMailer automatically detects whether the key being used for encryption is included in the user's Password list and allows to decrypt messages without any user interaction.

Key points

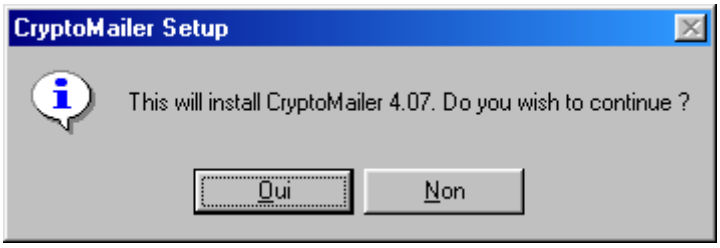
- Edit text messages & attach files
- Works with all mail clients available
- Integrated in the Windows environment (Drag&Drop, Context menu, etc.)
- User friendly key management, providing password protected key list
- 3DES and AES 128 bits encryption algorithm
- Compression
- Self-extracting file creation
- Automatically detects matching key (if present) in key list
- Supports multiple files
- Import / Export key lists
- Password protection (for running CryptoMailer)
- Key recovery and management tool for corporate users

© Sistech 1999 - 2003

2 Getting started

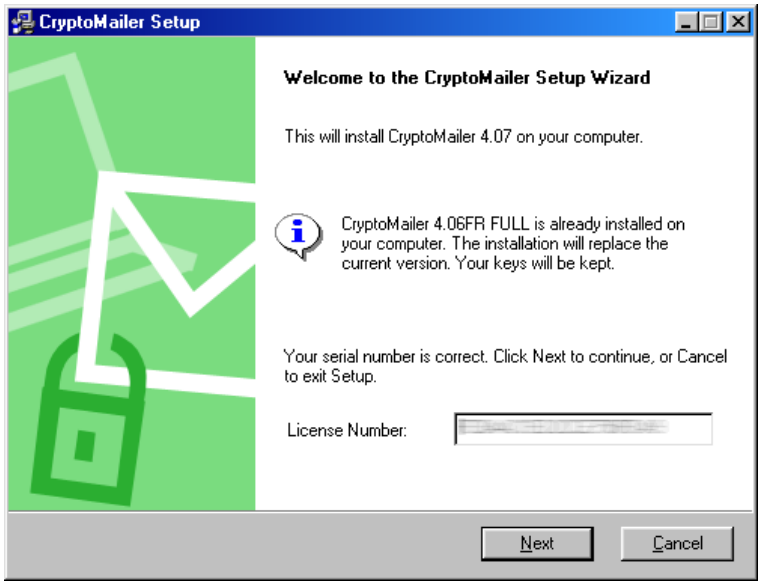
2.1 Installing

In order to install CryptoMailer, execute the install program (for example cmlfull407en.exe).



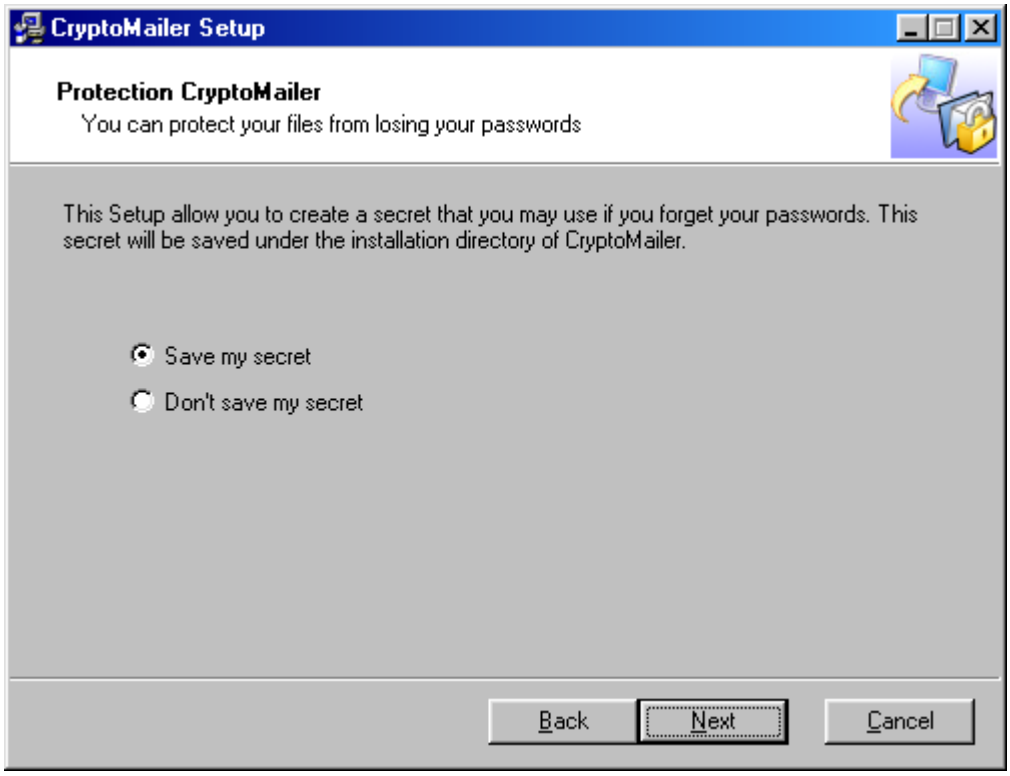
The install procedure is different, depending on the particular version of CryptoMailer you are installing (FULL, READER or FREE) : The FULL version requires a serial number to be provided by the user, which is not required by the READER and FREE versions.

The FULL version will automatically detect previously installed versions. Existing parameters and settings (key list, serial number, etc.) ; It will also keep existing Password lists from previously installed FREE or READER versions.


CryptoMailer Setup
Welcome to the CryptoMailer Setup Wizard
This will install CryptoMailer 4.07 on your computer.
CryptoMailer 4.06FR FULL is already installed on your computer. The installation will replace the current version. Your keys will be kept.
Your serial number is correct. Click Next to continue, or Cancel to exit Setup.
License Number:
Next
Cancel

The FULL version allows the user to generate a secret key to be used in combination with Cryptoboard for possible recovery after the loss of the Passphrases or of the key list. In order to be able to use recovery at any later moment, the secret key MUST be generated during installation, although the user is not obliged to do so. We highly recommend to take this precaution. No message can be recovered without this secret key. Cryptoboard alone (without the secret key generated during installation) does not provide any means for recovering encrypted messages.

© Sistech 1999 - 2003


CryptoMailer Setup
Protection CryptoMailer
You can protect your files from losing your passwords
This Setup allow you to create a secret that you may use if you forget your passwords. This secret will be saved under the installation directory of CryptoMailer.
Save my secret
Don't save my secret
Back
Next
Cancel

Users are free to generate the secret key or not. If the user decides to generate the secret key, it will be kept in a file located in the installation directory of CryptoMailer. It is encrypted with the serial number. It is HIGHLY RECOMMANDED to keep the secret key on a removable data support (diskette, USB memory stick, etc.) in a safe place.

Please contact our support team if you need to recover data after having lost your Passphrase.

2.2 Possible problems during installation

File already exists
During installation, a number of files are created by CryptoMailer. Sometimes, files can not be created because an older version of the same file already exists. A message will be displayed to the user (if that happens, it is likely to be the file « cryptmlr.dll »).

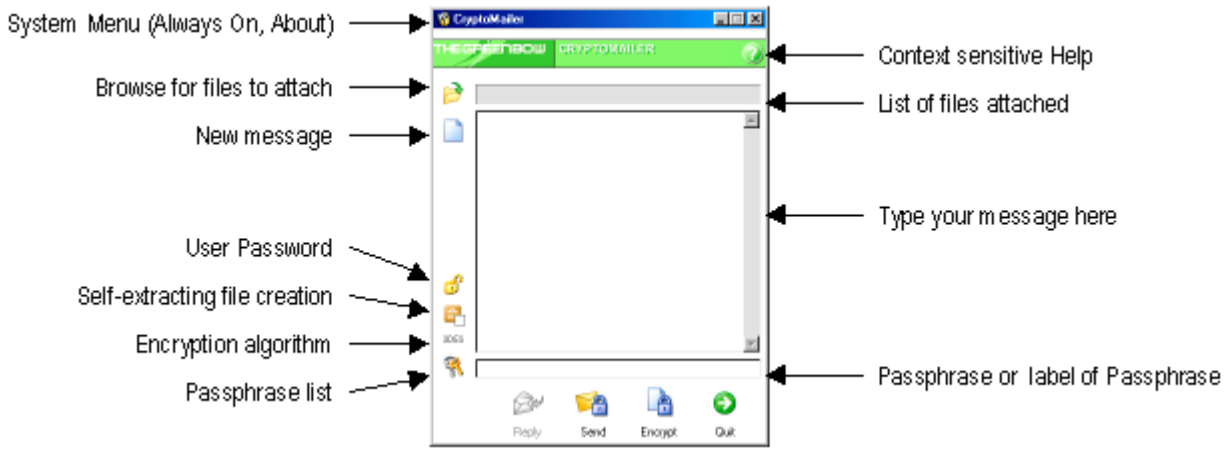
We recommend to Cancel the installation, delete the file manually and restart the installation.

© Sistech 1999 - 2003

3 How to use

3.1 CryptoMailer User Interface

The User Interface of CryptoMailer is divided in 3 major parts :



Editable fields
- List of files attached
- Message editor
- Password field

Buttons
- Encrypt and send message
- Select files to attach
- Password setup for User interface
- Self-extracting file creation
- Select encryption algorithm
- Passphrase management
- System menu

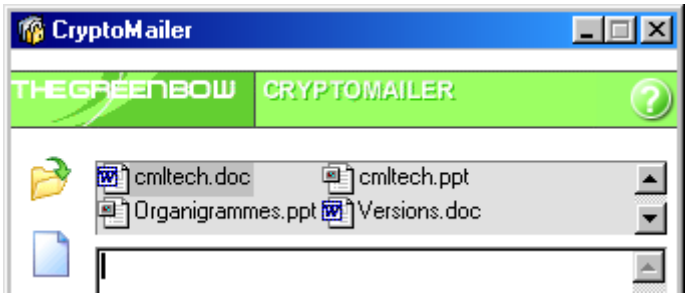
Direct access to CryptoMailer
- Drag and Drop files to encrypt / decrypt
- Context menu (right Mouse button) in the Explorer Window
- Double-click on encrypted file
- Upon reception of an encrypted e-mail

© Sistech 1999 - 2003

3.2 List of attached files

This list displays the names of the files to be encrypted (sending or encrypting local files) or being decrypted (receiving or decrypting local files).

The size of the window is adapting to the number of files attached.



A file can be added to the list by a Drag & Drop operation or by browsing for files using the Browser button

Note
When encrypting files locally (not sending them in an e-mail), files may be selected from different directories. Each file will be encrypted in it's original directory.

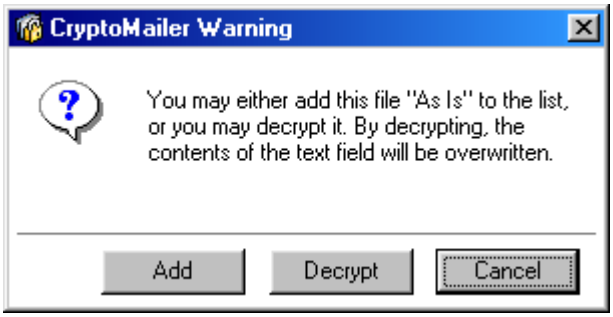
3.2.1 Right Mouse click and Double-click

Using the right mouse button with one of the files contained in the list, you may remove it from the list and (during decryption) open the file.
During decryption, double-clicking a file will open it.

3.2.2 Adding files that are already encrypted to the list

When a previously encrypted file is added to a list, CryptoMailer behaves as follows :
The new file is the first file to be added to the list. It will automatically be decrypted (using either an existing Passphrase from the list or prompting the corresponding Passphrase).
The new file is added to a list of previously unencrypted files. The User is offered two choices :

© Sistech 1999 - 2003


CryptoMailer Warning
You may either add this file "As Is" to the list, or you may decrypt it. By decrypting, the contents of the text field will be overwritten.
Add
Decrypt
Cancel

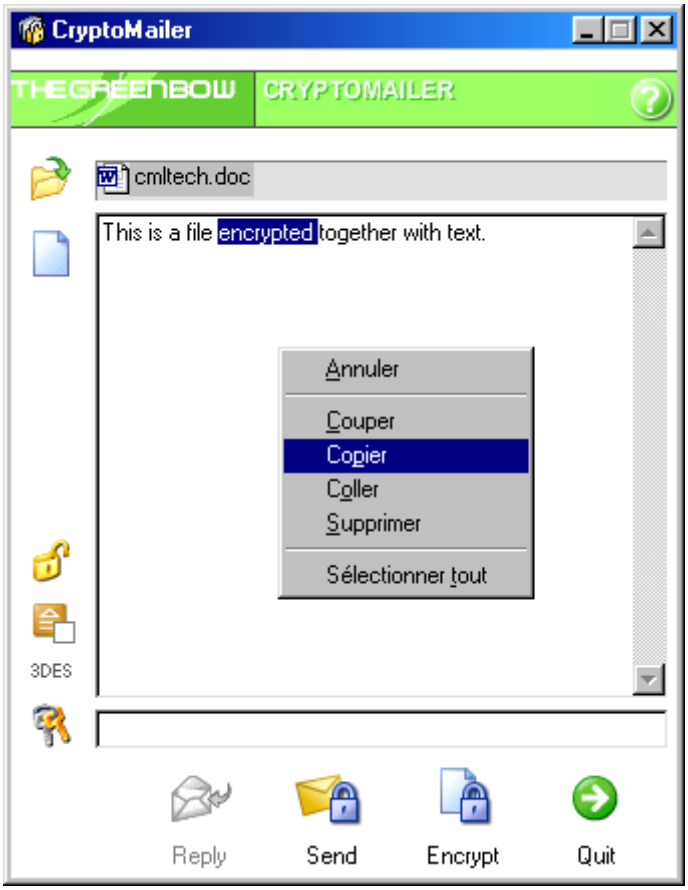
The user is free to either add the encrypted file to the list of files to be encrypted (the file will be re-encrypted) or decrypt the file. In the latter case, the file list will be replaced by the list of file contained in the newly decrypted file..

© Sistech 1999 - 2003

3.3 Message text field

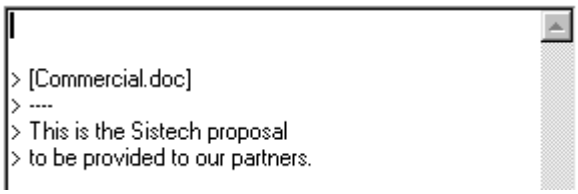
The message edit field allows to enter a text message (Memo) to be included in the encrypted file.
The message will be encrypted together with any attached files and « packed » into a single (compressed) end encrypted file.

The edit field provides all common editing features like (cut/copy/paste, etc.) and may receive text from the Clipboard (copied from another application like Notepad, Word, etc.).



The button allows to clear the message field and the file attachment list. After clearing the text field and the file list, CryptoMailer will be in « Encryption » mode (as opposed to « Decryption »).

By using the « reply » Button (respond to the currently open e-mail), the original text message will be indented and inserted into the reply text. The names of files attached to the original mail will also be displayed (the files will not be included !!).



© Sistech 1999 - 2003

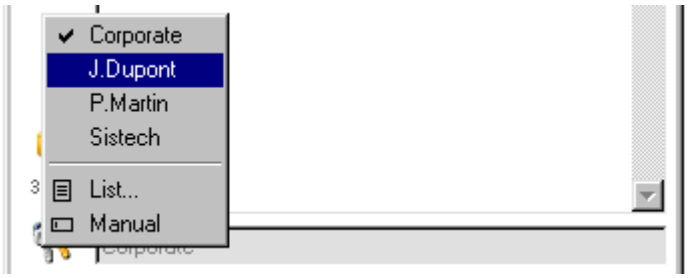
3.4 Entering a Passphrase

CryptoMailer is specially designed for ease-of-use and provides most comprehensive Passphrase management.

The Passphrase Management dialog is accessed by clicking on the button.

A menu will pop up, offering the following choices :

- A list of previously entered Passphrases, identified by their labels (identifiers) (The expressions displayed in the Passphrase list are only identifiers, NOT the Passphrases themselves).
- Access to the Passphrase List Management ("List").
- Switch to « manual » mode for entering the Passhrase. ("Manual").



3.4.1 Manual editing ("Manual")

By selecting this menu option, the user may manually enter a Passphrase in the Passphrase field. The Passphrase field allows to enter a maximum of 32 characters.

All characters are allowed to be used in the Passphrase field : Upper / lower case, numbers, special chars, accents, etc.. It is a common security criteria for defining Passwords / Passphrases, to use a mixture of chars, special chars and numbers as follows :

3.4.2 Passphrases and labels (identifiers)

CryptoMailer allows to register up to 32 different Passphrases. Once a Passphrase is entered and validated by the user, it may never be displayed again or recalled by any means. Each Passphrase is identified through a label defined by the user (usually identifying the target user / group). The Passphrase Management Menu is accessed through the menu item "List".

The Passphrase list provides rapid access to the predefined Passphrases, avoiding to re-type your Passphrase each time you send an encrypted message. It also provides automatic decryption support. Using a special algorithm, CryptoMailer checks all Passphrases contained in the list in order to find out whether one of them matches with the encrypted message. If a matching Passphrase is detected, it will automatically be used to decrypt the encrypted message / file.

3.4.3 Passphrase Management (« List... »)

The « List… » menu item opens the Passphrase List Management dialog.

Security rules for Passphrases :

© Sistech 1999 - 2003

In order to provide a reasonable level of privacy, some basic rules should always be respected when defining a new Passphrase :

❶ Use long expressions (at least 6 characters, 10 being a good average). The longer the Passphrase, the more possible combinations need to be checked by a potential Hacker.

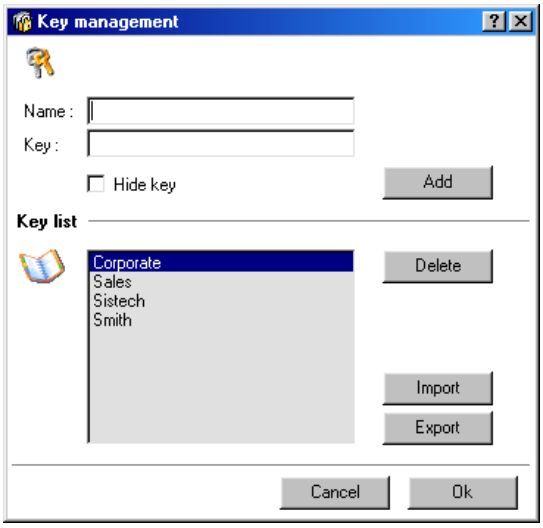
❷ Use combinations of upper / lower case characters, special characters (#, &, %, etc…), accents (é, à, ç, etc..) and numbers (Ex.: "this__?woud%°be)(-tricky\\979856"). This kind of Passphrase makes dictionary attacks useless and the only possible attack left is "Brute force", requiring literally Zillions of combinations.

❸ Avoid using expressions and names from your immediate social and professional environment (Birthday dates, street names, your kid's or relatives names, etc.). All these expressions are the first ones to be researched for by potential Hackers (especially if they are professionals). The way to obtain this information is called "social engineering" and a real Hacker wouldn't bother going through your Dustbin every Monday morning or hanging out in your favourite Pub or sitting next to you in the Subway, etc. Also avoid using the "Big Classics" like "Admin", "Administrator", "Password", "Default", "Root", etc.

© Sistech 1999 - 2003

3.5 Passphrase Management

The Passphrase Management Dialog allows to add, remove, import and export Passphrases.



Adding a Passphrase

1. Enter the label for the new Passphrase in the "Name" field. The label is used to identify the Passphrase for all subsequent operations. The Passphrase itself may never be displayed again.
   Usually, the label identifies the target person / group or organisation for encrypted communications.

2. Enter the Passphrase in the "Key" field.
   It is highly recommended to apply the basic security rules when defining a new Passphrase.
   It is possible to hide the Passphrase while typing. To do so, check the "Hide key" box.

3. Click on the Button "Add".

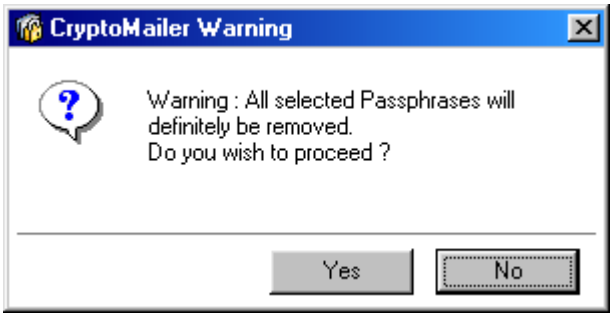
Note
The maximum number of Passphrases allowed is 32. If 32 Passphrases are contained in the list, the "Add" button is deactivated.

3.5.1 Removing a Passphrase

Select one or multiple Passphrases you wish to remove and click on the "Remove" button.

Attention
All selected Passhrases will definitely be removed. In order to avoid accidental removal of Passphrases, User confirmation is requested before the Passhrases are definitely deleted.

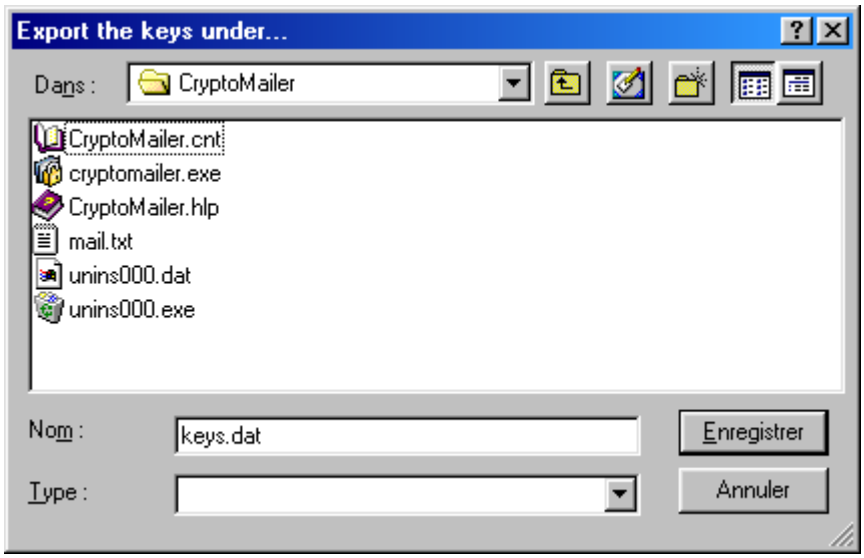
© Sistech 1999 - 2003



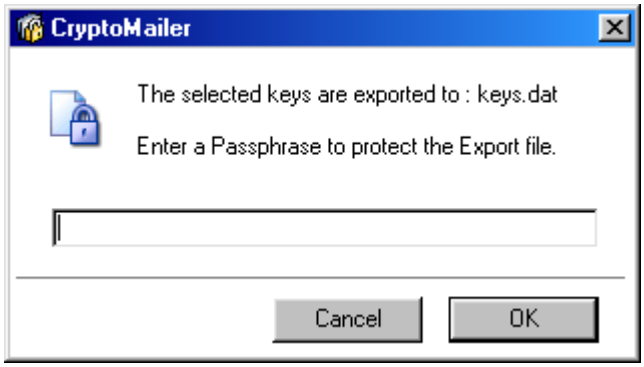
3.5.2 Exporting Passphrases

CryptoMailer allows to export Passphrases for backup or transmission.
The Exported Passphrase file is encrypted. Therefore, it may safely be transmitted by e-mail !

Select the Passphrases you wish to export and click on the "Export" button. CryptoMailer will prompt you for a destination directory and filename (see dialog below), as well as a Passphrase to be used for encrypting the Export file :



© Sistech 1999 - 2003



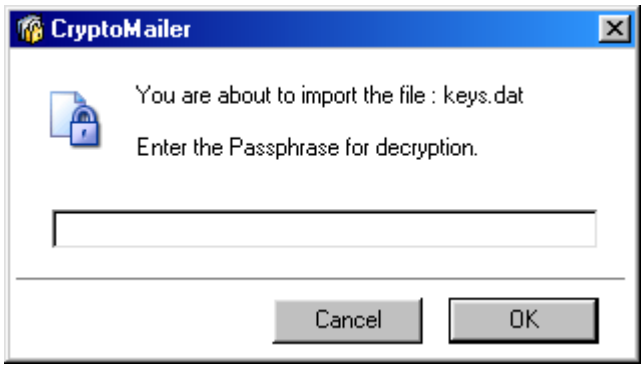
Remember to apply the basic rules for specifying a Passphrase.

Attention
In order to avoid accidental exportation of the entire list of Passphrases, CryptoMailer prompts for User confirmation before creating the Export file :

Note
The Password List may not be exported neither in the FREE version nor in the READER version of CryptoMailer.

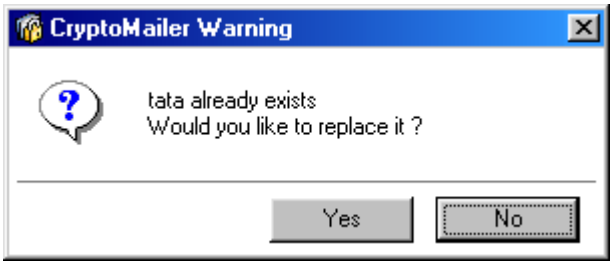
3.5.3 Importing Passphrases

CryptoMailer allows to import Passphrase Export files generated by CryptoMailer. The generated files are not compatible with any other product on the market.
To import a Passphrase file, click on "Import", browse and select the file and click OK.
CryptoMailer prompts for the Passphrase in order to decrypt the Export file.



© Sistech 1999 - 2003

The imported Passphrases are added to the list of existing Passphrases. While importing, CryptoMailer checks for redundancy and prompts the user whenever it encounters a conflict with an existing entry :



Note
The FREE version of CryptoMailer does not include the "Import" feature.

© Sistech 1999 - 2003

3.6 Encrypt and Send

The primary task buttons of CryptoMailer are located at the bottom of the Main Dialog.
The buttons change states depending on the operating mode of CryptoMailer.

In "Encryption" mode, the user may :
- send an encrypted message ("Send" button)
- locally encrypt one or several files ("Encrypt" button).

In "Decryption" mode, the user may
- decrypt the files attached to a temporary location for viewing the contents ("Open" Button).
- permanently decrypt an attached file ("Decrypt" Button).
- immediately respond to an encrypted message via an encrypted reply ("Reply" Button)

3.6.1 Sending an encrypted e-mail

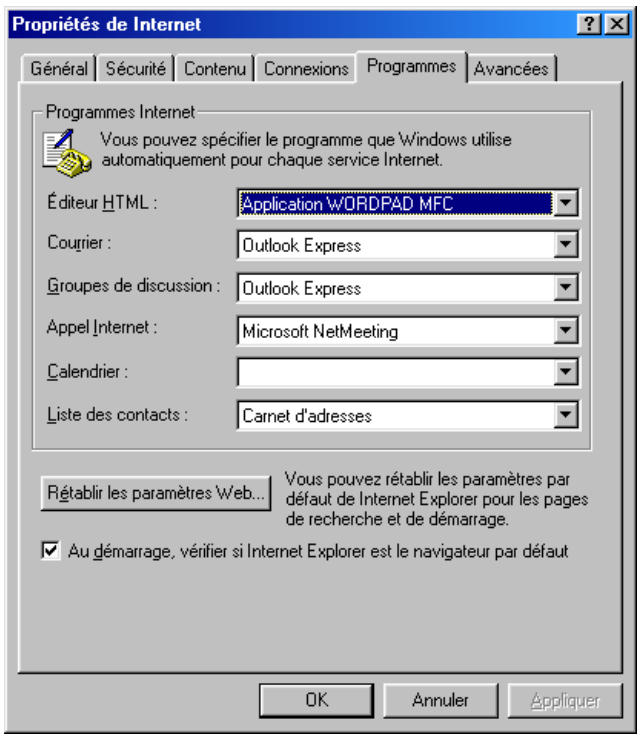
When clicking the "Send" Button, the attached files and the message text are concatenated, compressed and formatted into a single encrypted message. CryptoMailer then opens the default e-mail client of the current user and automatically creates a new outgoing message containing the encrypted data as a file attachment. The user simply selects the destination e-mail address and sends the message as usual.

The text of the message body (as in the screenshot above) can be changed anytime. It is stored in the file "mail.txt" which can be found in the install directory of CryptoMailer.

© Sistech 1999 - 2003

Note

The e-mail client called by CryptoMailer is always the default e-mail client of the current user. In order to change the e-mail client, open the Control Panel, click on "Internet Options" and select the "Programs" tab. Select your default e-mail client in the "mail" field.:



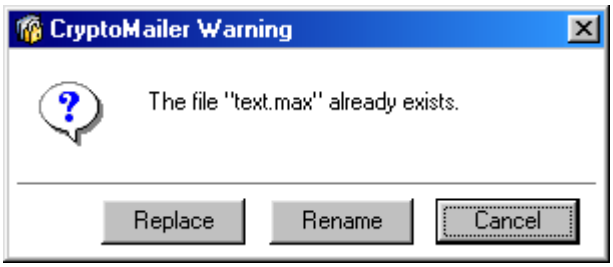
3.6.2 Encrypt locally

When selecting the "encrypt" button, each file contained in the list of attached files will be encrypted in its own directory and a new encrypted file is generated. (ex. If 10 files are contained in the list, 10 encrypted files will be generated). If any text was entered in the message field, it will be encrypted and stored in a file named "text.max".

The file "text.max" will automatically be placed in the same directory as the first file in the list – if at least one file is contained in the list.

If no file is contained in the list (empty list), CryptoMailer prompts the user to chose the destination directory, thus allowing the user to use CryptoMailer for taking confidential notes rapidly and safely.

If any of the output (encrypted) files generated by CryptoMailer already exits, CryptoMailer asks whether to rename the newly generated file or to replace the existing file by the new one.:



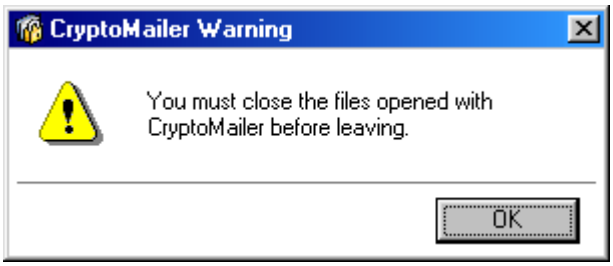
© Sistech 1999 - 2003

Note
CryptoMailer does not encrypt complete directories.

3.6.3 Temporary decryption (Open)

When selecting the "Open" button, the file selected in the file list is immediately decrypted and opened (similar to double-clicking a file in Explorer).

Note
The file being opened temporarily for viewing its contents will be stored in a temporary Windows directory. In order not to leave any unencrypted information on the harddrive, CryptoMailer tries to erase the temporary file asap. Therefore, simple text files (.txt extension) are deleted right after decrypting and displaying. A .doc (Word) document can only be erased after Word was closed. Therefore, CryptoMailer can not be closed as long as there are open documents being viewed by the user.:



3.6.4 Decrypt locally

By clicking the "Decrypt" button, all files contained in the attached files list (as well as any text contained in the message window) are decrypted and stored in
- in the same directory as the encrypted file,
- in a directory to be selected by the user in case of an encrypted file received by mail.

3.6.5 Replying to an encrypted mail

When an encrypted file is received by e-mail, the "Reply" button is activated.
The user may then reply directly, using the same Passphrase that had been used to decrypt the message. Naturally, the user may select a different Passphrase for the reply mail.

After clicking the "Reply" button, the Message editing Window contains the original message text indented with "> " and the name(s) of the file(s) attached to the original mail.

© Sistech 1999 - 2003

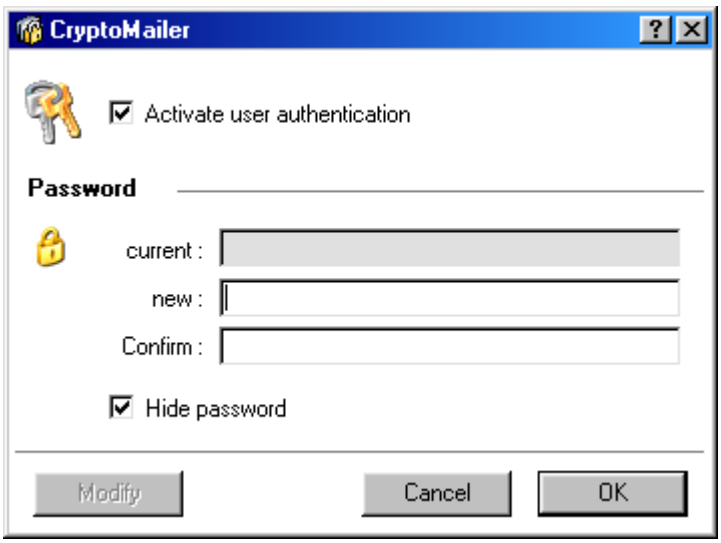
3.7 User authentication

It is possible to lock the access to CryptoMailer with a Password.

If other people have access to your computer, you may want to lock access to CryptoMailer, so they cannot open and read your secret files and messages.

The Password protection is activated by clicking on the icon.

The configuration dialog for the access lock feature is shown below. It allows to define a Password or to replace an existing one. It is highly recommended to apply the rules for specifying safe Passwords (see above).

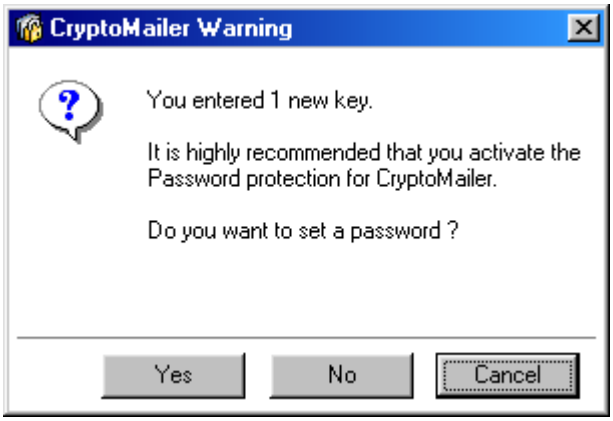


The "Modify" button is only active, if the Password protection has been activated before. The field "Current" is activated once the user clicks on the "Modify" button. The Password characters may be hidden (replaced by stars) by checking the "Hide Password" button.

When Password protection is active, the icon becomes .

Note
Activating the Password protection for CryptoMailer aims to protect the User's Passphrase list (used for en/decryption). Therefore, CryptoMailer automatically suggests to activate Password protection as soon as at least one Passphrase has been entered in the list.

© Sistech 1999 - 2003


CryptoMailer Warning
You entered 1 new key.
It is highly recommended that you activate the Password protection for CryptoMailer.
Do you want to set a password ?
Yes
No
Cancel

Warning

The Password can not be recovered after being set up. In case you lose or forget the Password protecting the access to CryptoMailer, you will need to re-install CryptoMailer – and loose all the Passphrases possibly contained in the list.

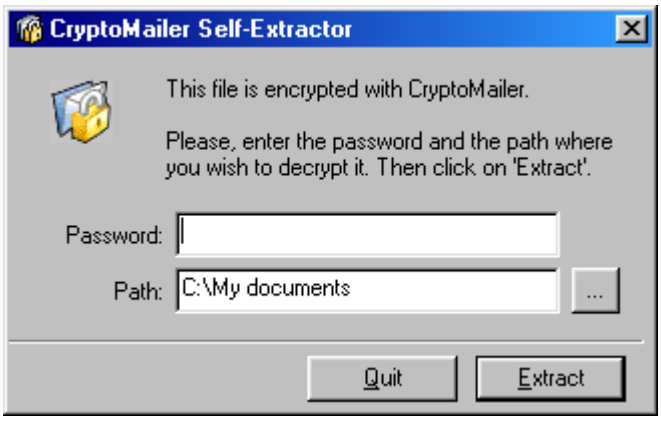
© Sistech 1999 - 2003

3.8 Self-Extracting File

Cryptomailer optionally allows to create self-extracting files.

In order to send an encrypted e-mail as a self-extracting message, activate the icon before sending the mail. Cryptomailer will then generate a self-extracting mail ("file.exe").

Upon reception of a self-extracting message, the user will be prompted to enter the password required for decryption and to select the target directory for the extracted files.



Note : Since CryptoMailer READER cannot process encryption, this feature is not available with CryptoMailer READER. The icon is disabled.

© Sistech 1999 - 2003

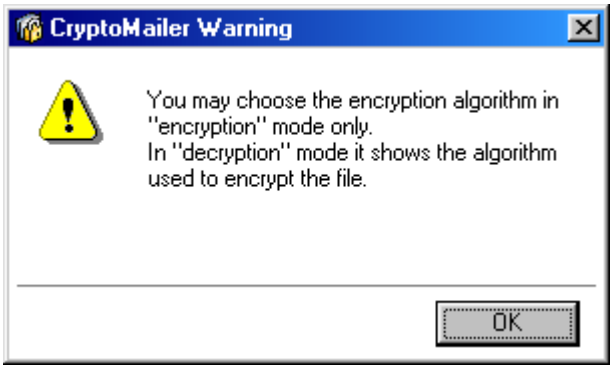
3.9 Encryption algorithms

CryptoMailer supports 2 cryptographic algorithms : AES or DES.

The FREE version of CryptoMailer operates with a key length of 56 bits (AES or DES).
The FULL version of CryptoMailer operates with a key length of 128 bits (AES or 3DES 112 bits).

In order to select / change the encryption algorithm, click on the 3DES icon in the main Window :

During decryption, CryptoMailer automatically detects the algorithm used for encryption. Therefore, the user is not requested to select manually during decryption. Clicking on the "Algorithm" icon will produce the following message :


CryptoMailer Warning
You may choose the encryption algorithm in "encryption" mode only.
In "decryption" mode it shows the algorithm used to encrypt the file.
OK

What exactly is a "encryption algorithm"?
An encryption algorithm (or cryptographic algorithm) consists of several mathematical operations allowing to transform a "readable" message into an "unreadable" message. Most cryptographic algorithms require a user-defined key to be included in the operation.

Cryptographic algorithms can be classified regarding speed of execution, key length (the longer the keys, the better the encryption), underlying mathematical theories (symmetric / asymmetric, elliptic curve, etc) and whether they are public or secret.

DES,3DES et AES are symmetric algorithms, meaning that the secret key being used for encryption is the same as the one that has to be used for decryption. Therefore, the Passphrases used with CryptoMailer must be shared between the sender and the receiver of an encrypted message. If several Passphrases need to be shared by a group of users, the Export / Import feature of CryptoMailer is very useful.

© Sistech 1999 - 2003

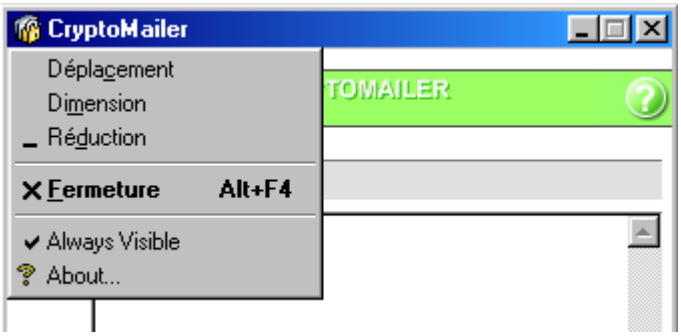
CryptoMailer is compliant to official cryptographic standards. It generates a new random key for each encryption being performed. The same file being encrypted several times using the same Passphrase will always produce a different output file (containing the encrypted data). The random key generation is compliant to PKCS#5.

CryptoMailer uses the hashing algorithm MD5 for calculating signatures and of encrypted files and Passphrases.

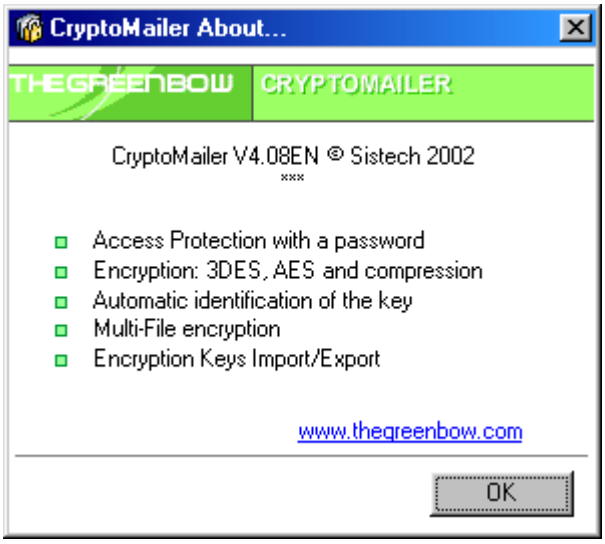
© Sistech 1999 - 2003

3.10 System menu

The system menu is accessible through a Mouse-click on the icon in the Title Bar.



Besides the standard Windows functions, it allows to make CryptoMailer always visible (remaining on top of all other Windows) and gives access to the "About" Dialog which contains version information and provides a link to the Thegreenbow Website.



© Sistech 1999 - 2003

3.11 Drag and Drop

CryptoMailer provides Drag and Drop support for encrypting or decrypting files. Simply drag a file from any Windows location to the CryptoMailer Window and drop it anywhere.

If the dropped file is an encrypted file, it will automatically be decrypted and the message text and the list of files contained will be displayed.

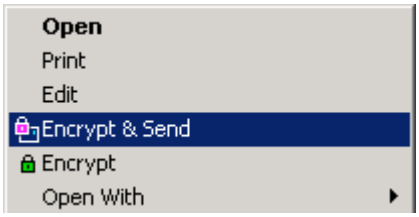
If the Passphrase that was used for encrypting the dropped file is contained in the list of Passphrases of CryptoMailer, decryption will be fully automatic and the user will not be prompted for a Passphrase.

If the dropped file is not encrypted (for example a ".doc" or ".xls" file), it will be added to the list of files attached.

© Sistech 1999 - 2003

3.12 Context Menu

CryptoMailer can be accessed through the Context Menu of Explorer by right-clicking on a selected file or a group of files. CryptoMailer is adding two Menu items to the Context Menu : "Encrypt & send" and "Encrypt". Right-clicking on n encrypted file will offer the option "Decrypt".



"Encrypt" and "Encrypt & send" will open CryptoMailer with the selected files being added to the list of files attached.

"Decrypt" opens CryptoMailer and displays the message text and the list of the files attached. If the encrypted file is a file that was encrypted locally (not sent or received as a mail message), CryptoMailer will simply decrypt it and replace the encrypted (".max") file by the unencrypted file (the original file).

Note
The Context menu items are not available with the free "Reader" version of CryptoMailer.
Currently, CryptoMailer does not handle multiple encrypted files selected. The user will be receive a Warning message instead.
CryptoMailer does not identify encrypted files by the file extension (".max"), but by the file's contents. Therefore, the encrypted files can be renamed by the user "at will".

3.13 Receiving an encrypted file

Upon reception of an encrypted message, opening the attached file will automatically launch CryptoMailer and display the message text and the list of files included.

If the Passphrase that was used for encrypting the mail is contained in the list of Passphrases, CryptoMailer will automatically decrypt the message without prompting the user.

The "Reply" button automatically gets activated.

© Sistech 1999 - 2003

3.14 Opening an encrypted file

A double-click on an encrypted file automatically opens the file with CryptoMailer.

If the Passphrase that was used for encrypting the mail is contained in the list of Passphrases, CryptoMailer will automatically decrypt the file without prompting the user.

Note
If access to the Workstation is not protected, it is highly recommended to activate Password protection for CryptoMailer.

3.15 Problems with encrypting files

CryptoMailer may not be able to encrypt in the following cases :

1. if there is a problem with system resources (lack of memory, etc.) or CryptoMailer internal resources (corrupted Passphrase files, etc.). The user will receive a Warning message.

2. CryptoMailer was installed in the free READER version, allowing only to decrypt files or messages, but not to encrypt.

© Sistech 1999 - 2003

4 Uninstalling

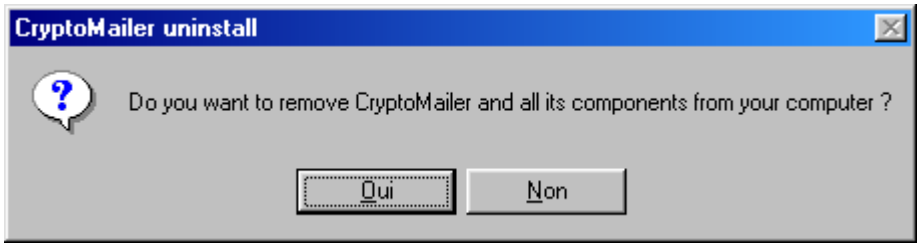
CryptoMailer can be uninstalled through the "Start" Menu or the Windows Control Panel :

4.1 Start Menu

- Select "Programs", "Thegreenbow", "CryptoMailer" and "Uninstall CryptoMailer".

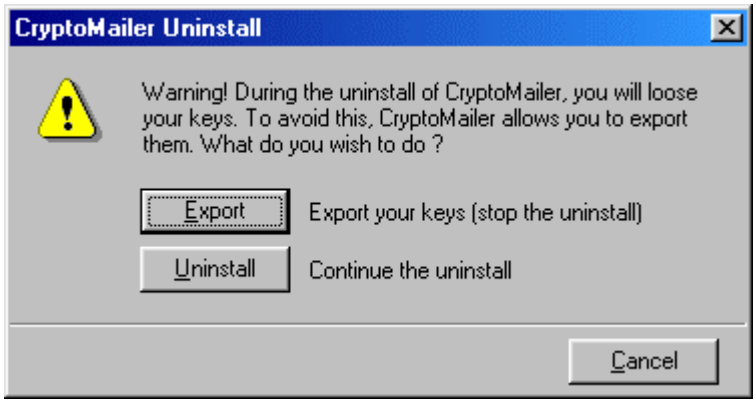
4.2 Control Panel

- Open the Windows Control Panel
- Select "Add/Remove Programs".
- Select "CryptoMailer [...]" and click on the "Add/Remove" Button...
- Click "OK".



If you are running CryptoMailer FULL, the uninstall program prompts about a potential loose of your keys. You can :

- Continue the uninstall without a backup of your key list ("Uninstall" button)
- Stop the uninstall program and export your key list ("Export" button) : the uninstall program will automatically launch CryptoMailer on the 'key export' window.
- Cancel the uninstall program (exit without any action).


CryptoMailer Uninstall
Warning! During the uninstall of CryptoMailer, you will loose your keys. To avoid this, CryptoMailer allows you to export them. What do you wish to do ?
Export
Export your keys (stop the uninstall)
Uninstall
Continue the uninstall
Cancel

© Sistech 1999 - 2003

5 CryptoBoard

5.1 Introduction

Cryptoboard is a Windows application allowing to customize CryptoMailer. It also provides support for asymmetric key recovery. Cryptoboard also allows to customize the Title Bar and the Bitmap logo..

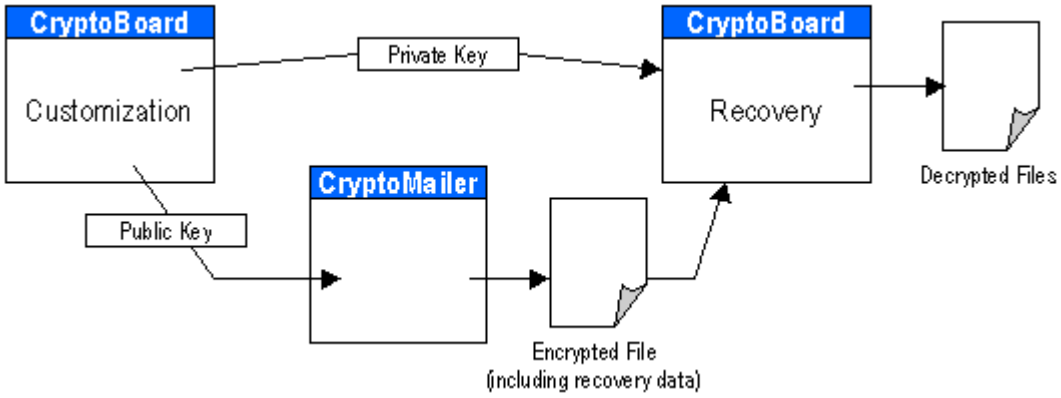
Key recovery is a necessary feature for corporate customers with regards to legal issues and potential loss of information.

Additional information about Cryptoboard is available online at : www.thegreenbow.fr.

5.2 Mechanisms

The key recovery mechanism provided by CryptoMailer is based on asymmetric encryption mechanisms :

❶ **CryptoBoard** allows to generate a key pair (private key associated to a public key)
❷ The public key is injected into the executable CryptoMailer.exe file (which will be distributed to the user within the corporation). The private key is safely stored and must be kept in a secure location by one or several security managers. The private key can be "cut into pieces" and distributed to a number of people, requiring that for example 3 out of 5 people must provide their part of the key in order to proceed to a recovery operation.
❸ Recovery of encrypted messages or files can be performed with CryptoBoard only, in combination with the private key.



© Sistech 1999 - 2003

6 Contacts

CryptoBoard™ and **CryptoMailer™** are part of the **TheGreenBow®** product line, developed by **Sistech S.A.**

Support

E-mail : support@thegreenbow.com
Web : http://www.thegreenbow.fr/support.html
Tél. : +33.1.43.12.39.30

Information

E-mail : info@thegreenbow.com
Web : http://www.thegreenbow.fr
Tél. : +33.1.43.12.39.37

Sistech S.A.
28 rue de Caumartin
75009 Paris
France

© Sistech 1999 - 2003